

CLAIMS

Amend the claims as follows.

1. (Currently Amended) A method, comprising:
locating a steganographic program comprising executable code that includes ~~both read and write~~ software calls that introduce steganographic items into a computer file;
obtaining a steganographic signature by reading a partial section of the executable code ~~, wherein the steganographic program is configured to introduce steganographic items into a computer file via the software calls~~;
identifying, with a processing device, computer files comprising software code;
obtaining one or more test signatures by reading partial sections of the software code;
comparing the steganographic signature with the one or more test signatures; and
displaying a listing of which of the computer files comprise the test signatures that provide a match with the steganographic signature.
2. (Currently Amended) The method according to claim ~~Claim~~ 1, wherein the listing includes an identification of a location of the steganographic items ~~location~~ in a computer system.
3. (Cancelled)
4. (Currently Amended) The method according to claim ~~Claim~~ 1, wherein the executable code comprises a dynamic link library (DLL) file.
5. (Currently Amended) The method according to claim ~~Claim~~ 1, wherein certain of the computer files that comprise an asserted file type are excluded when comparing the one or more test signatures with the steganographic signature.
6. (Currently Amended) The method according to claim ~~Claim~~ 1, further comprising:

checking a respective real file type by reading a start of the ~~one or more~~ computer files;
and
excluding files having prearranged initial byte sequences from the comparison.

7. (Cancelled)

8. (Currently Amended) The method according to claim Claim 1, wherein the ~~one or more~~ computer files comprise deleted files.

9. (Currently Amended) The method according to claim Claim 1, wherein the ~~one or more~~ computer files comprise self-extracting executable files.

10. (Currently Amended) The method according to claim Claim 1, wherein some prearranged files are not identified in the listing despite containing code which matches the steganographic signature.

11. (Currently Amended) ~~A computer~~ An apparatus comprising a storage device for storing one or more computer files, wherein the ~~computer~~ apparatus is configured to:

obtain a steganographic signature by reading a partial section of executable code of a program, wherein the program includes ~~both read and write~~ software calls that introduce steganographic items into a computer file;

identify ~~identifying~~ the one or more computer files comprising software code;

obtain ~~obtaining~~ one or more test signatures by reading partial sections of the software code;

compare the steganographic signature with the one or more test signatures; and

when a match with the steganographic signature is found, indicate ~~indicating~~ which of the one or more computer files provide the match.

12. (Currently Amended) The apparatus according to claim Claim 11, wherein the indication incorporates an identification of the steganographic signature.

13. (Cancelled)
14. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein the steganographic signature comprises a continuous sequence of the partial section of the executable code.
15. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein one or more predetermined file types are not compared with the steganographic signature.
16. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein the partial section of the executable code comprises a start of the program, and wherein files having prearranged initial byte sequences are excluded from the comparison.
17. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein files not accessible by a system administrator are excluded from the comparison.
18. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein the one or more computer files comprise logical wastebasket files.
19. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein the one or more computer files comprise polymorphic files.
20. (Currently Amended) The apparatus according to claim ~~Claim~~ 11, wherein one or more predetermined files are not indicated despite containing the software code which matches the steganographic signature.
21. (Cancelled)
22. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein the operations further comprise identifying a steganographic item responsible for the match.

23. (Cancelled)

24. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein the steganographic signature comprises a continuous sequence of executable program code but not more than 5% and not less than 0.167% of the program.

25. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein an asserted file type is not compared with the steganographic signature.

26. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein the operations further comprise:

checking a real file type by reading a start of the one or more computer files; and
excluding files having prearranged initial byte sequences from the comparison.

27. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein files that are not accessible by a system administrator are excluded from the comparison.

28. (Currently Amended) The non-transitory computer readable medium according to claim ~~Claim~~ 31, wherein the one or more computer files comprise logical wastebasket files.

29. (Cancelled)

30. (Currently Amended) The computer readable medium according to claim ~~Claim~~ 31, wherein the operations further comprise displaying the one or more computer files that provide the match, and wherein files associated with certain file types are not displayed despite containing code which matches the steganographic signature.

31. (Currently Amended) A non-transitory ~~tangible~~ computer readable medium having stored therein computer readable instructions that, in response to execution by a system, cause the system to perform operations comprising:

- identifying one or more computer files comprising software code;
- obtaining one or more test signatures by reading partial sections of the software code;
- obtaining a steganographic signature by reading executable code comprising part of a program including software calls that introduce ~~capable of introducing~~ steganographic items into the one or more computer files;
- comparing the steganographic signature with the one or more test signatures; and
- identifying the one or more computer files associated with the one or more test signatures that provide a match with the steganographic signature.

32. (Currently Amended) The non-transitory computer readable medium according to claim 31, wherein the operations further comprise executing the one or more files, and wherein the comparison is made prior to executing the one or more files.

33. (Previously Presented) The method according to claim 1, further comprising running a virus checking program while comparing the steganographic signature with the one or more test signatures.

34. (Previously Presented) The apparatus according to claim 15, wherein the one or more predetermined file types comprise a graphic editor.

35. (Cancelled)

36. (Currently Amended) The ~~computer~~ apparatus according to claim 11, wherein the ~~computer~~ apparatus is further configured to analyze the one or more test signatures with a virus checking program in combination with the comparison with the steganographic signature.

37. (Currently Amended) The non-transitory computer readable medium according to claim 31, wherein the operations further comprise:

identifying a plurality of steganographic programs including both read and write software calls that introduce the steganographic items; and

obtaining a plurality of steganographic signatures associated with the steganographic programs for comparison with the one or more test signatures.

38. (Cancelled)

39. (New) The method according to claim 1, wherein the executable code comprises both read and write software calls that introduce the steganographic items.